REMARKS

This is intended as a full and complete response to the Final Office Action dated September 21, 2007, having a shortened statutory period for response set to expire on December 21, 2007. Applicants submit this response to place the application in condition for allowance or in better form for appeal. Please reconsider the claims pending in the application for reasons discussed below.

Claims 1-17 and 20-53 are pending in the application. Claims 1-17 and 20-53 remain pending following entry of this response. Applicants submit that the amendments and new claims do not introduce new matter.

Claim Rejections - 35 U.S.C. § 103

Claims 1-17 and 20-53 are rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent No. 7,149,311 to *MacKenzie et al.* in view of U.S. Patent No. 6,975,204 to *Silver.* Applicants respectfully traverse this rejection.

The Examiner bears the initial burden of establishing a *prima facie* case of obviousness. *See* MPEP § 2142. To establish a *prima facie* case of obviousness three basic criteria must be met. First, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one ordinary skill in the art, to modify the reference or to combine the reference teachings. Second, there must be a reasonable expectation of success. Third, the prior art reference (or references when combined) must teach or suggest all the claim limitations. *See* MPEP § 2143. The present rejection fails to establish at least the first criteria.

For example, *MacKenzie* in view of *Silver*, does not disclose a "method for disabling on-demand resources on a computerized apparatus" that includes "disabling at least one on-demand resource of the computerized apparatus, thereby rendering the disabled on-demand resource unavailable for use by users of the computerized apparatus, wherein the disabled on-demand resource is a hardware resource of the computerized apparatus," as recited by claim 1. Independent claims 9, 20, 31, 36, 38, 46, and 47 each recite a similar limitation.

MacKenzie is directed to a technique for protecting access to a cryptographic "private key." As is well known, a "private key" provides one of two keys used in asymmetric cryptography. The private key can be used to decrypt data that has been encrypted using the public key, which is shared with all involved parties. The private key is also used to "sign" outgoing messages. "Signing" typically involves encrypting the message (or a hash of the message) using the private key. Because the public key is shared, anyone can then decrypt the message (or the hash) to verify that the message was, in fact, "signed" with the private key. Because the private key can be used to "sign" messages, a compromised key may be used impersonate the rightful key-holder. Similarly, a comprised private key may be used to access messages, documents, etc. encrypted with the public key. Ultimately, the private key and public key are simply two large numbers related to one another in a particular way. Also, the private key and public key are typically represented as hexadecimal values.

Because of the obvious security issues related to the private key, a number of techniques have been developed to safeguard the security thereof. For example, the private key is usually encrypted with an asymmetric key, i.e., a key that may be used to both encrypt and decrypt information. Typically, the asymmetric key is expressed as a user password. However, this leaves the private key open to a "dictionary attack," i.e., an attack of simply guessing every possible password until finding the correct one. Given these known security vulnerabilities of a private key, *MacKenzie* discloses a technique for "key disabling," by which "the rightful owner of a stolen device can disable the device's private key even if the attacker already knows the user's password." *Mackenzie*, Abstract. That is, *MacKenzie* discloses a means to revoke a compromised private key, to prevent the use of a revoked key in cryptographic operations.

In rejecting claim 1, 8, and 31, the Examiner suggests:

> As per claims 1, 8, and 31, *MacKenzie* discloses the disabling of a key-utilizing resource via an encrypted user disablement command generated from inputted authorization codes issued via a remote server, which is executed after it is verified (authenticated) (see column 6, lines 43-48).

Office Action, p. 2. The passage cited by the Examiner provides:

628146_1

> In the key disabling type of protocol of the invention, the user can issue a request to the server to disable future use of the private key associated with the device's public key. Once the server receives this request and verifies it is well-formed, the device's key is rendered useless to the attacker, even if the attacker knows the user's password.

MacKenzie, 6:43-48. Stated differently, once the server verifies a request to revoke a private key, the server will refuse to allow the use of that key (e.g., for message signing and decrypting). Note, the cryptographic mathematics still function using both the password and the private key, but the server will nevertheless refuse to use the private key in any requested cryptographic operations.

Based on the foregoing, it should be clear that *Mackenzie* does not disclose "disabling at least one on-demand resource, thereby rendering the disabled on-demand resource unavailable for use by users of the computerized apparatus." Rather, *MacKenzie* discloses a technique for revoking the validity of a private key, of a private public key pair, in order to prevent a comprised private key from being used in cryptographic operations "even if the attacker knows the user's password." Thus, no "on-demand resources on a computerized apparatus" are disabled in the private-key revocation. Accordingly, Applicants respectfully request that the rejection of independent claims 1, 9, 20, 31, 36, 38, 46, and 47. Further, Applicants submit that dependent claims 2-8, 10-16, 21-30, 32-35, 37, 39-45, and 48-53 are allowable as well.

Therefore, the claims are believed to be allowable, and allowance of the claims is respectfully requested.

628146_1

Conclusion

Having addressed all issues set out in the office action, Applicants respectfully submit that the claims are in condition for allowance and respectfully request that the claims be allowed.

If the Examiner believes any issues remain that prevent this application from going to issue, the Examiner is strongly encouraged to contact Gero McClellan, attorney of record, at (336) 643-3065, to discuss strategies for moving prosecution forward toward allowance.

Respectfully submitted, and
S-signed pursuant to 37 CFR 1.4,

/Gero G. McClellan, Reg. No. 44,227/

Gero G. McClellan
Registration No. 44,227
PATTERSON & SHERIDAN, L.L.P.
3040 Post Oak Blvd. Suite 1500
Houston, TX 77056
Telephone: (713) 623-4844
Facsimile: (713) 623-4846
Attorney for Applicants